

ПРОГНОЗИРОВАНИЕ ВЕРОЯТНОСТИ УСПЕШНОЙ СПУФИНГОВОЙ АТАКИ В ЛОКАЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ

С.А. Князьков

Филиал НИЦ Телеком в городе Самаре, г. Самара

Ключевые слова: локальная вычислительная сеть, информационная безопасность, спуфинговая атака, задержка распространения пакета

Методы проведения атак в локальных вычислительных сетях столь же разнообразны, как и цели, которые достигаются с помощью таких атак [1].

Спуфинговые атаки – это целый класс различного рода атак, основывающихся на особенности многих сетевых протоколов, работающих по типу запрос-ответ [2]. Такие атаки являются наиболее опасными, так как спектр их применения наиболее широк [3]. Зачастую успешность спуфинговой атаки зависит от задержки времени распространения сетевого пакета от узла назначения к узлу источнику.

В связи с вышеописанной проблемой, было проведено исследование влияния сетевой инфраструктуры, в частности количества сетевых узлов на пути от отправителя до получателя, на задержки сетевых пакетов для решения задачи прогнозирования спфинговых сетевых атак.

Для выполнения поставленной задачи было проведено экспериментальное исследование и проанализированы обработанные данные с помощью визуальных средств представления информации в виде графиков и гистограмм. Пример гистограммы распределения задержек сетевых пакетов изображён на рисунке 1.

Исходя из характера гистограмм была аппроксимирована функция вероятности задержек. Для этого использовалось некоторое количество s парциальных нормальных функций плотностей $f_i^s(t)$ для i -го расстояния. Проинтегрировав, просуммировав и умножив на соответствующие весовые коэффициенты парциальные функции плотностей была получена формула функции распределения задержек распространения для i -го расстояния:

$$F_i(t) = \frac{1}{N \cdot n_i} \sum_{s=1}^N \left(\int_0^t f_i^s(t) dt \cdot w_s \right),$$

где N – количество парциальных законов распределения, из которых строится плотность распределения задержек;

$f_i^s(t)$ – парциальная плотность распределения задержек для i -го расстояния;

w_s – вектор весовых коэффициентов парциальных функций распределения;

n_i – нормирующий коэффициент функции распределения задержек для i -го

расстояния.

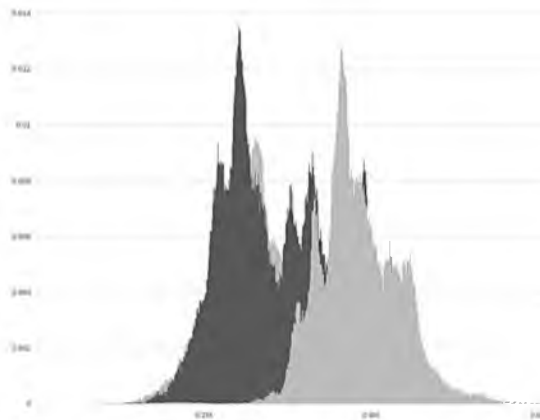


Рисунок 1 - Пример распределения задержек сетевых пакетов в ходе проведения экспериментальных исследований

Таким образом, при правильном расчёте или подборе коэффициентов, можно с достаточной точностью аппроксимировать функцию распределения и плотности задержек.

Наконец, с помощью формул 1 и 2 была рассчитана вероятность успешной спуфинговой атаки в зависимости от разницы сетевого расстояния между атакующим и атакуемым узлами.

$$P_{\Delta} = \frac{1}{M - |\Delta|} \sum_{i=1}^M \sum_{j=1}^M \begin{cases} P_{ij}, & j - i = \Delta \\ 0, & \text{иначе} \end{cases} \quad (1)$$

где Δ – разница расстояний между атакующим и атакуемым;

P_{Δ} – вероятность успешной атаки для разницы расстояний между атакующим и атакуемым;

P_{ij} – вероятность успешной атаки для i -го расстояния атакуемого и j -го расстояния атакующего;

M – полное сетевое расстояние.

$$P_{ij} = \max_t \left(\sqrt{(1 - F_i(t)) \cdot F_j(t)} \right) \quad (2)$$

где P_{ij} – вероятность успешной атаки для i -го расстояния и j -го расстояния;

$F_i(t)$ – функция распределения задержек распространения для i -го расстояния;

$F_j(t)$ – функция распределения задержек распространения для j -го расстояния.

Графики зависимости вероятности успешной атаки от взаимного

расположения, атакующего и атакуемого узлов для экспериментальных данных и смоделированных данных представлены на рисунке 2.

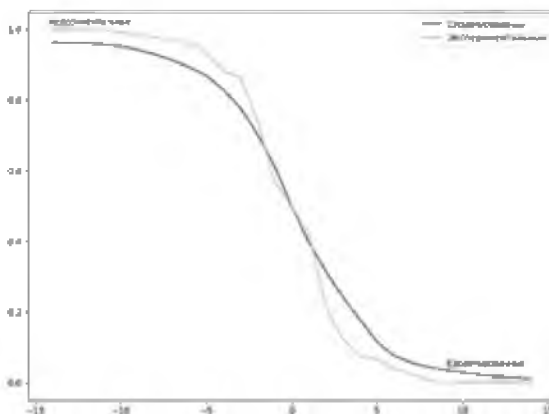


Рисунок 2 - Сравнение модели на основе экспериментальных данных

Для оценки точности модели была рассчитана ошибка аппроксимации по алгоритму среднеквадратичного отклонения, которая составила 0.078.

Список использованных источников

1. Олифер, В. Компьютерные сети. Принципы, технологии, протоколы [Текст]/В. Олифер, Н. Олифер. – СПб.: Питер, 2021.-1008 с.
2. Дэвис, Р. Искусство тестирования на проникновение в сеть [Текст]/Р. Дэвис. – М.: ДМК Пресс, 2021.-310 с.
3. Макаренко, С.И. Защита компьютерных сетей и телекоммуникаций [Текст]: учебное пособие/С.И. Макаренко. – СПб.: Научно-технические технологии, 2024.-311 с

Князьков Сергей Александрович, инженер 2 категории, филиал НИЦ Телеком в г. Самаре, knyazkovsa@nic-t.ru

УДК 004.056.57, 004.054

ПРИМЕНЕНИЕ ФУНКЦИИ РАСПРЕДЕЛЕНИЯ ВРЕМЕННЫХ ЗАДЕРЖЕК РАСПРОСТРАНЕНИЯ ПАКЕТА В ЛОКАЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ ДЛЯ АНАЛИЗА ВЕРОЯТНОСТИ УСПЕШНОЙ СПУФИНГОВОЙ АТАКИ

С.А. Князьков

Филиал НИЦ Телеком в городе Самаре, г. Самара

Ключевые слова: локальная вычислительная сеть, информационная безопасность, сетевая атака, задержка распространения пакета